بسمه تعالی

☐ دفاع از رساله دکتری ☐ سمینار عمومی (Colloquium)

■ دفاع از پایان‌نامه کارشناسی‌ارشد ☐ سمینار تخصصی (Seminar)

☐ سمینار تخصصی و مشورتی (Informal Seminar)

عنوان : رمزنگاری تصویر با استفاده از الگوریتم AES موازی بر روی GPU

سخنران : سیامک وطنی

چکیده:

با توجه به رشد سریع ارتباطات چندرسانه‌ای و پخش گسترده اطلاعات تصویری، امنیت اطلاعات تصویر بسیار حائز اهمیت می‌باشد. رمزنگاری تصویر به علت کاربردهای متنوع آن در کاربردهای تجاری، نظامی، پزشکی و... به یکی از حوزه‌های فعال و پویا تبدیل‌شده است. در رمزنگاری تصویر به دلیل ویژگی‌هایی نظیر حجم بالا، نیازهای فشرده‌سازی اطلاعات، محدودیت‌های منابع محاسباتی پردازنده، محدودیت‌های پهنای باند شبکه، وابستگی شدید اطلاعات پیکسل‌ها به هم‌زمان پاسخ در کاربردهای بلادرنگ و...، روش‌های رمزنگاری سنتی نظیر: AES، DES و IDEA به علت سرعت کم و ماهیت وابسته اطلاعات تصویری قابل‌استفاده نمی‌باشند. دومین مشکل طول کلید رمزنگاری می‌باشد. با توجه به حجم زیاد داده‌ها و استفاده از روش‌های سنتی موجب محدود شدن طول کلید شده و اطلاعات رمز شده به‌شدت در معرض آسیب‌پذیری در برابر حملات نوع متن رمز شده می‌باشند.

در سال‌های اخیر الگوریتم‌های زیادی بر اساس روش‌هایی نظیر نگاشت آشوب، تبدیل فوریه کسری، اتوماتای سلولی، دنباله‌های DNA و ... ارائه‌شده است.

با معرفی GPU که برای عملیات پردازش موازی ابزار کارآمدی محسوب می‌شود، سرعت پردازش گرافیکی، کیفیت تصویر و اجرای نرم‌افزارهای گرافیکی به‌شدت افزایش یافت. در این پایان‌نامه با توجه به ساختار داده‌ای تصویری یک الگوریتم رمزنگاری AES موازی مناسب برای رمز کردن داده‌های حجیم و منطبق با معماری GPU، اصلاح و پیاده‌سازی شده است. با توجه به آنکه پیکسل‌های یک تصویر به‌شدت به هم وابسته‌اند این رمزنگاری به‌گونه‌ای پیاده‌سازی شده که ضمن استفاده از قابلیت پردازش موازی GPU برای افزایش کارایی به‌گونه‌ای تغییر یابد تا دو مفهوم پخش و گمراه‌کنندگی نیز لحاظ شوند. با این رویکرد ضمن تغییر مشخصه آماری تصویر که آن را در برابر حملات مقاوم می‌کند، تصویر به‌شدت درهم‌ریخته شده و ازنظر بصری بدون توجه به ساختار آن غیرقابل تشخیص می‌شود.

کلمات کلیدی: AES، GPU، نظریه آشوب، رمزنگاری تصویر و پردازش موازی

زمان برگزاری: ۹۵/۱۲/۲۵

مکان برگزاری: دانشکده مهندسی و علوم کامپیوتر